CLAIMS

1. A computer controlled method to construct a secure credential infrastructure comprising steps of:

exchanging key commitment information over a preferred channel between a credential issuing device and a prospective member device to pre-authenticate said prospective member device;

receiving a public key from said prospective member device;

verifying said public key with said key commitment information; and

automatically provisioning said prospective member device with a credential authorized by a credential issuing authority.

2. The computer controlled method of claim 1, further comprising establishing proof that said prospective member device is in possession of a private key corresponding to said public key.

3. The computer controlled method of claim 2, further comprising establishing a communication channel between said prospective member device and said credential issuing authority responsive to the step of establishing proof.

4. The computer controlled method of claim 3, wherein said credential is secret and said communication channel is a secure communication channel.

5. The computer controlled method of claim 1, further comprising configuring said credential issuing authority.

6. The computer controlled method of claim 1, wherein said credential issuing device includes said credential issuing authority.

7. The computer controlled method of claim 1, wherein the step of exchanging further comprises sending network configuration information to said prospective member device.

8. The computer controlled method of claim 1, wherein the step of automatically provisioning further comprises steps of:

determining provisioning information for said prospective member device; and

sending said provisioning information to said prospective member device.

9. The computer controlled method of claim 8, wherein said provisioning information further comprises application-specific configuration information.

10. The computer controlled method of claim 1, wherein said preferred channel is a location-limited channel.

11. The computer controlled method of claim 1, wherein said preferred channel uses a telephone switching system.

12. The computer controlled method of claim 1, wherein said preferred channel has a demonstrative identification property and an authenticity property.

13. The computer controlled method of claim 1, wherein said key commitment information is selected from one or more of the group consisting of a portion of said public key, said public key, an encoding of said public key, and a mathematical function of said public key.

14. The computer controlled method of claim 1, wherein the step of automatically provisioning is performed by said credential issuing device.

15. The computer controlled method of claim 1, wherein the step of automatically provisioning is performed by an enrollment station in communication with said credential issuing device.

16. The computer controlled method of claim 15, wherein the method further comprises establishing secure communication between said enrollment station and said credential issuing device.

17. The computer controlled method of claim 1, wherein said prospective member device is selected from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.

18. The computer controlled method of claim 1, wherein said secure credential infrastructure is a public key infrastructure, said credential issuing authority is a certification authority and said credential is a public key certificate.

19. The computer controlled method of claim 18, wherein the step of automatically provisioning further comprises steps of:

determining provisioning information for said prospective member device;

creating a public key certificate as said credential responsive to said provisioning information; and

sending said public key certificate to said prospective member device.

20. The computer controlled method of claim 18, wherein the step of exchanging further comprises steps of:

creating a public key pair for said prospective member device; and

sending said public key pair to said prospective member device over said preferred channel.

21. The computer controlled method of claim 18, further comprises steps of:

creating a trusted key pair;

storing said trusted key pair;

establishing a certification authority public key certificate; and

storing said certification authority public key certificate.

22. The computer controlled method of claim 21, wherein the step of automatically provisioning is responsive to authorization from a registration agent.

23. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to construct a secure credential infrastructure, the method comprising steps of:

exchanging key commitment information over a preferred channel between a credential issuing device and a prospective member device to pre-authenticate said prospective member device;

receiving a public key from said prospective member device;

verifying said public key with said key commitment information; and

automatically provisioning said prospective member device with a credential authorized by a credential issuing authority.

24. The computer-readable storage medium of claim 23, wherein said public key is received over said preferred channel.

25. The computer-readable storage medium of claim 23, wherein the step of automatically provisioning further comprises steps of:

determining provisioning information for said prospective member device; and

sending said provisioning information to said prospective member device.

26. The computer-readable storage medium of claim 23, wherein the step of exchanging is initiated by said prospective member device.

27. The computer-readable storage medium of claim 23, wherein the step of exchanging is initiated by said credential issuing device.

28. The computer-readable storage medium of claim 23, wherein the step of automatically provisioning is performed by said credential issuing device.

29. The computer-readable storage medium of claim 23, wherein said prospective member device is selected from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.

30. The computer-readable storage medium of claim 23, wherein said secure credential infrastructure is a public key infrastructure, said credential issuing authority is a certification authority and said credential is a public key certificate.

31. A credential issuing apparatus configured to construct a secure credential infrastructure comprising:

at least one port configured to establish a preferred channel;

a key commitment receiver mechanism configured to receive key commitment information through said at least one port;

a key receiver mechanism configured to receive a public key;

a pre-authentication mechanism configured to verify said public key with said key commitment information; and

a credential provisioning mechanism configured to be able to automatically provide a credential authorized by a credential issuing authority responsive to the pre-authentication mechanism.

32. The apparatus of claim 31, wherein said public key is received over said preferred channel.

33. The apparatus of claim 31, further comprising a key-pair validation mechanism configured to establish proof that a prospective member device is in possession of a private key corresponding to said public key.

34. The apparatus of claim 31, further comprising an initialization mechanism configured to configure said credential issuing authority.

35. The apparatus of claim 31, wherein said credential issuing device further comprises said credential issuing authority.

36. The apparatus of claim 31, further comprises a network device configuration mechanism configured to send network configuration information over said preferred channel.

37. The apparatus of claim 31, wherein the credential provisioning mechanism further comprises:

a determination mechanism configured to determine provisioning information for said prospective member device; and

a transmission mechanism configure to send said provisioning information to said prospective member device.

38. The apparatus of claim 31, wherein said key commitment information is selected from the group consisting of a portion of said public key, said public key, an encoding of said public key, and a mathematical function of said public key.

39. The apparatus of claim 31, wherein the credential issuing device is an enrollment station capable of being in communication with said credential issuing authority.

40. The apparatus of claim 33, wherein said prospective member device is selected from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.

41. The apparatus of claim 31, wherein said secure credential infrastructure is a public key infrastructure, said credential issuing authority is a certification authority and said credential is a public key certificate.

42. The apparatus of claim 41, wherein the credential provisioning mechanism further comprises:

a services determination mechanism capable of determining provisioning information for a prospective member device;

a certificate creation mechanism configured to create a public key certificate as said credential responsive to said provisioning information; and

a sending mechanism capable of sending said public key certificate to said prospective member device.

43. The apparatus of claim 41, wherein the key commitment receiver mechanism further comprises:

a key creation mechanism capable of creating a public key pair for a prospective member device; and

a sending mechanism capable of sending said public key pair to said prospective member device over said preferred channel.

44. The apparatus of claim 41, further comprising an automatic configuration mechanism comprising:

a key pair creation mechanism configured to create a trusted key pair;

a key pair storage mechanism configured to store said trusted key pair;

a public key certificate generation mechanism configured to establish a certification authority public key certificate responsive to said trusted key pair; and

a certificate storage mechanism configured to store said certification authority public key certificate.

45. The apparatus of claim 44, wherein the public key certificate generation mechanism further comprises a parent CA receiver mechanism configured to receive said certification authority public key certificate from a parent certification authority.

46. A credential issuing apparatus configured to construct a secure credential infrastructure comprising:

at least one port configured to establish a preferred channel;

a key commitment receiver mechanism configured to receive commitment information for a secret through said at least one port;

a key receiver mechanism configured to receive said secret;

a pre-authentication mechanism configured to verify said secret with said commitment information; and

a credential provisioning mechanism configured to be able to automatically provide a credential authorized by a credential issuing authority responsive to the pre-authentication mechanism.

47. A computer controlled method to join a prospective member device with a secure credential infrastructure comprising steps of:

exchanging key commitment information over a preferred channel between a credential issuing device and said prospective member device;

receiving a public key by said prospective member device;

verifying said public key with said key commitment information; and

receiving a credential authorized by a credential issuing authority.

48. The computer controlled method of claim 47, further comprising establishing proof that said credential issuing device is in possession of a private key corresponding to said public key.

49. The computer controlled method of claim 48, further comprising establishing a communication channel between said prospective member device and said credential issuing authority responsive to the step of establishing proof.

50. The computer controlled method of claim 47, wherein said secure credential infrastructure is a public key infrastructure, said credential issuing authority is a certification authority and said credential is a public key certificate.

51. The computer controlled method of claim 47, wherein said preferred channel is a location-limited channel.

52. The computer controlled method of claim 47, wherein said preferred channel uses a telephone switching system.

53. The computer controlled method of claim 47, wherein said preferred channel has a demonstrative identification property and an authenticity property.

54. The computer controlled method of claim 47, wherein the step of exchanging is initiated by said prospective member device.

55. The computer controlled method of claim 47, wherein the step of exchanging is initiated by said credential issuing device.

56. The computer controlled method of claim 47, wherein said key commitment information comprises a portion of said public key.

57. The computer controlled method of claim 47, wherein said key commitment information comprises a function of said public key.

58. The computer controlled method of claim 50, further comprising receiving a public key pair by said prospective member device.

59. The computer controlled method of claim 47, further comprising receiving provisioning information by said prospective member device.

60. The computer controlled method of claim 47, wherein said prospective member device is selected from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.

61. A computer-readable storage medium storing instructions that when executed by a computer cause the computer to join a prospective member device with a secure credential infrastructure, the method comprising steps of:

exchanging key commitment information over a preferred channel between a credential issuing device and said prospective member device;

receiving a public key by said prospective member device;

verifying said public key with said key commitment information; and

receiving a credential authorized by a credential issuing authority.

62. The computer-readable storage medium of claim 61, wherein said preferred channel uses a telephone switching system.

63. The computer-readable storage medium of claim 61, wherein the step of exchanging is initiated by said prospective member device.

64. The computer-readable storage medium of claim 61, wherein the step of exchanging is initiated by said credential issuing device.

65. The computer-readable storage medium of claim 61, wherein said key commitment information comprises a function of said public key.

66. The computer-readable storage medium of claim 61, wherein said prospective member device is selected from one or more of the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.

67. An apparatus capable of joining a secure credential infrastructure comprising:

at least one port configured to establish a preferred channel;

a key commitment receiver mechanism configured to receive key commitment information though said at least one port;

a key receiver mechanism configured to receive a public key;

a pre-authentication mechanism configured to verify said public key with said key commitment information; and

a credential receiving mechanism configured to receive a credential responsive to the pre-authentication mechanism.

68. The apparatus of claim 67, further comprising a key-pair validation mechanism configured to establish proof that a credential issuing device is in possession of a private key corresponding to said public key.

69. The apparatus of claim 68, further comprising a network interface configured to establish a communication channel with a credential issuing authority responsive to the key-pair validation mechanism.

70. The apparatus of claim 67, wherein said secure credential infrastructure is a public key infrastructure, said credential issuing authority is a certification authority and said credential is a public key certificate.

71. The apparatus of claim 67, wherein said preferred channel is a location-limited channel.

72. The apparatus of claim 67, wherein said preferred channel has a demonstrative identification property and an authenticity property.

73. The apparatus of claim 67, wherein said key commitment information comprises a portion of said public key.

74. The apparatus of claim 67, wherein said key commitment information comprises a function of said public key.

75. The apparatus of claim 70, further comprising a receiving mechanism capable of receiving a public key pair.

76. The apparatus of claim 67, further comprising a receiving mechanism capable of receiving provisioning information.

77. The apparatus of claim 67, further including one or more components selected from the group consisting of a computer, a personal data assistant, a smart card, a cryptographic token, a medical device, a device containing personal information, a secure telephone, a cell telephone, a vehicle, a container, an access card, a biometric sensor, a wireless network device, a proximity sensor, a sensor device, traffic sensor, an alarm device, a robot, a device capable of receiving a credential, a device capable of issuing a credential.